iPhone and iPod touch
Enterprise Deployment Guide

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

Simultaneously published in the United States and Canada.

019-1333/2008-07

Contents

iPhone in the Enterprise

Learn how to integrate iPhone and iPod touch with your enterprise systems.

This guide is for system administrators. It provides information about deploying and supporting iPhone and iPod touch in enterprise environments.

System Requirements

Read this section for an overview of the system requirements and the various components available for integrating iPhone and iPod touch with your enterprise systems.

iPhone and iPod touch

iPhone and iPod touch devices you use with your enterprise network must be updated with iPhone software 2.0 or later.

iTunes

iTunes 7.7 or later is required in order to set up a device. This version is also required in order to install software updates for iPhone or iPod touch, install applications, as well as to sync music, video, or other data with a Mac or PC.

To use iTunes, you need a Mac or PC that has a USB 2.0 port and meets the following specifications.

Mac OS X computers

- Mac OS X v10.4.10 Tiger or later
- 1 GHz processor or faster
- 256 MB of RAM
- QuickTime 7.1.6 or later

Windows computers

- Windows XP Service Pack 2 or Windows Vista
- 500 MHz Pentium processor or faster
- 256 MB of RAM
- QuickTime 7.1.6 or later

Some features of iTunes, such as use of the iTunes Store, have additional requirements. See the documentation included with the iTunes installer for more information.

iPhone Configuration Utility

iPhone Configuration Utility lets you create configuration profiles for your devices.

The Mac OS X version of the utility also lets you manage profiles, install applications, and view console logs from connected devices. This version requires:

- Mac OS X v10.5 Leopard

The web-based version of the utility requires:

- Microsoft Windows Vista (32-bit only), or Microsoft Windows XP with .NET Framework Version 2.0, or Mac OS X v10.5 Leopard
- Microsoft Internet Explorer 7, or Firefox 2, or Safari 3

Microsoft Exchange ActiveSync

iPhone and iPod touch support the following versions of Microsoft Exchange:

- Exchange ActiveSync for Exchange Server (EAS) 2003 Service Pack 2
- Exchange ActiveSync for Exchange Server (EAS) 2007 Service Pack 1

Supported Exchange ActiveSync Policies

The following Exchange policies are supported:

- Enforce password on device
- Minimum password length
- Require both numbers and letters
- Inactivity time in minutes

For a description of each policy, refer to your Exchange ActiveSync documentation.

Remote Wipe

You can remotely wipe the contents of an iPhone or iPod touch. Doing so quickly removes all data and configuration information from the device, then the device is securely erased and restored to original, factory settings. It can take approximately one hour for each 8 GB of device capacity for the process to finish.

With Exchange Server 2007, you can initiate a remote wipe using the Exchange Management Console, Outlook Web Access, or the Exchange ActiveSync Mobile Administration Web Tool.

With Exchange Server 2003, you can initiate a remote wipe using the Exchange ActiveSync Mobile Administration Web Tool.

Users can also wipe a device in their possession by choosing Erase All Content and Settings from the Settings menu.

Important: Because wiping the device can take a long time, connect the device to its power supply. If the device turns off due to low power, the wiping process resumes when the device is connected to power.

Microsoft Direct Push

The Exchange server delivers email, contacts and calendar events to iPhone automatically if a cellular data connection is available. With iPod touch, or when iPhone doesn't have a cellular data signal, information isn't automatically pushed to the device; it's retrieved when you try to view the data or when you choose Settings > Fetch New Data.

Microsoft Exchange Autodiscovery

The Autodiscovery service of Exchange Server 2007 is supported. When you're manually configuring an iPhone and iPod touch, the Autodiscovery service uses your email address and password to automatically determine the correct Exchange server information.

Microsoft Exchange Global Address List

iPhone and iPod touch retrieve contact information from your company's Exchange server corporate directory. You can access the directory when searching in Contacts, and it is automatically accessed for completing email addresses as you enter them.

Exchange ActiveSync Features Not Supported

Not all Exchange features are supported, including, for example:

- Folder management
- Opening links in email to documents stored on Sharepoint servers
- Task synchronization
- Setting an "out of office" autoreply message
- Creating meeting invitations
- Flagging messages for follow-up

VPN

iPhone and iPod touch work with VPN servers that support the following protocols and authentication methods:

- L2TP/IPSec with user authentication by MS-CHAPV2 Password, RSA SecurID and CryptoCard, and machine authentication by shared secret.
- PPTP with user authentication by MS-CHAPV2 Password, RSA SecurID, and CryptoCard.
- Cisco IPSec with user authentication by Password, RSA SecurID, or CryptoCard, and machine authentication by shared secret and certificates. See Appendix A for recommendations for configuring Cisco VPN servers.

Network Security

iPhone and iPod touchiPod touch support the following 802.11i wireless networking security standards as defined by the Wi-Fi Alliance:

- WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

Additionally, iPhone and iPod touch support the following 802.1X authentication methods for WPA Enterprise and WPA2 Enterprise networks:

- EAP-TLS
- EAP -TTLS
- EAP-FAST
- PEAP v0, PEAP v1
- LEAP

Certificates

iPhone and iPod touch can use certificates in the following raw formats:

- PKCS1 (.cer, .crt, .der)
- PKSC12 (.p12, .pfx)

Email accounts

iPhone and iPod touch support industry-standard IMAP4- and POP3-enabled mail solutions on a range of server platforms including Windows, UNIX, Linux, and Mac OS X.

Additional Resources

In addition to this guide, the following publications and websites provide information about iPhone and iPod touch:

- *iPhone User Guide*, available for download at www.apple.com/support/iphone
- iPhone Guided Tour at www.apple.com/iphone/gettingstarted
- iPod touch Guided Tour at www.apple.com/ipodtouch/guidedtour
- iPhone webpage at www.apple.com/iphone
- iPod touch webpage at www.apple.com/ipodtouch
- iPhone in Enterprise webpage at www.apple.com/iphone/enterprise
- iPhone Support webpage at www.apple.com/support/iphone
- iPod touch Support webpage at www.apple.com/support/ipodtouch
- iTunes webpage at www.apple.com/itunes
- Exchange Product Overview at http://technet.microsoft.com/en-us/library/bb124558.aspx
- Exchange 2003 Technical Documentation Library at http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx
- Wi-Fi for Enterprise webpage at www.wi-fi.org/enterprise.php

Deploying iPhone and iPod touch 1

This chapter provides an overview of how to deploy iPhone and iPod touch in your enterprise.

iPhone and iPod touch are designed to easily integrate with your enterprise systems including Microsoft Exchange 2003 and 2007, 802.1X-based secure wireless networks, and Cisco IPSec virtual private networks. As with any enterprise solution, good planning and an understanding of your deployment options make deployment easier and more efficient for you and your users.

When planning your deployment of iPhone and iPod touch consider the following:

- How will your company's iPhones be activated for wireless cellular service?
- Which enterprise network services, applications and data will your users need to access?
- What policies do you want to set on the devices to protect sensitive company data?
- Do you want to manually configure devices individually, or use a streamlined process for configuring a large fleet?

The specifics of your enterprise environment, IT policies, wireless carrier, and your computing and communication requirements affect how you tailor your deployment strategy.

Activating Devices

Each iPhone must be activated with your wireless carrier before it can be used to make and receive calls, send text messages or connect to the cellular data network. Contact your carrier for voice and data tariffs and activation instructions for consumer and business customers.

You or your user will need to install a SIM card in the iPhone. After the SIM card is installed, iPhone must be connected to a computer with iTunes to complete the activation process. If the SIM card is already active, iPhone will be unlocked and ready for immediate use; otherwise, iTunes will walk you through the process of activating a new line of service.

Although there is no cellular service or SIM card for iPod touch, it must also be connected to a computer with iTunes for unlocking.

Because iTunes is required to complete the activation process for both iPhone and iPod touch, you must decide whether you want to install iTunes on each user's Mac or PC, or whether you'll complete activation for each device with your own iTunes installation.

After activation, iTunes isn't required to use the device with your enterprise systems, but it is necessary to synchronize music, video and web browser bookmarks with a computer. It is also required for downloading and installing software updates for devices and installing your enterprise applications. For more information, see Chapter 4.

Preparing Access to Network Services and Enterprise Data

iPhone 2.0 software enables secure push email, push contacts and push calendar with your existing Microsoft Exchange Server 2003 or 2007 solution, as well as Global Address Lookup, Remote Wipe and device passcode policy enforcement. It also allows users to securely connect to company resources via WPA Enterprise and WPA2 Enterprise wireless networks using 802.1X wireless authentication and/or via VPN using PPTP, LT2P over IPSec, or Cisco IPSec protocols.

If your company doesn't use Microsoft Exchange, your users can still use iPhone or iPod touch to wirelessly sync email with most standard POP or IMAP-based servers and services. And they can use iTunes to sync calendar events and contacts from Mac OS X iCal and Address Book or Microsoft Outlook on a Windows PC.

As you determine which network services you want users to access, here are some things you should know:

Microsoft Exchange

iPhone communicates directly with your Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS). Exchange ActiveSync maintains a connection between the Exchange Server and iPhone so that when a new email message or meeting invitation arrives iPhone is instantly updated. iPod touch doesn't have a cellular connection, so it receives push notifications only when it is active and connected to a Wi-Fi network.

If your company currently supports Exchange ActiveSync on Exchange Server 2003 or Exchange Server 2007, you already have the necessary services in place, no additional configuration is required.

If you have an Exchange Server but your company is new to Exchange ActiveSync, review the following:

Network Configuration

- Make sure port 443 is open on the firewall. If your company uses Outlook Web Access, port 443 is most likely already open.
- Verify that a server certificate is installed on the Exchange frontend server and enable Require Basic SSL for the Exchange ActiveSync virtual directory.
- On the Microsoft Internet Security and Acceleration (ISA) Server, verify that a server certificate is installed and update the public DNS to properly resolve incoming connections.
- Make sure the DNS for your network returns a single, externally-routable address to the Exchange ActiveSync server for both intranet and Internet clients. This is required so the device can use the same IP address for communicating with the server when both types of connections are active.
- On the ISA Server, create a web listener as well as an Exchange web client access publishing rule. This is a necessary step in enabling Exchange ActiveSync. See Microsoft's documentation for details.
- For all firewalls and network appliances, set the idle session timeout to 30 minutes. Refer to Microsoft Exchange documentation for alternative heartbeat and timeout intervals.

Exchange Account Setup

- Enable Exchange ActiveSync for specific users or groups using the Active Directory service. These are enabled by default for all mobile devices at the organizational level in Exchange Server 2003 and Exchange Server 2007. For Exchange Server 2007, see Recipient Configuration in the Exchange Management Console.
- Configure mobile features, policies, and device security settings using the Exchange System Manager. For Exchange Server 2007, this is done in the Exchange Management Console.
- Download and install the Microsoft Exchange ActiveSync Mobile Administration Web Tool, which is necessary to initiate a remote wipe. For Exchange Server 2007, remote wipe can also be initiated using Outlook Web Access.

WPA/WPA2 Enterprise Wi-Fi Networks

Support for WPA Enterprise and WPA2 Enterprise ensures that corporate wireless networks are securely accessed on iPhone and iPod touch. WPA/WPA2 Enterprise uses 128-bit encryption, a proven block-based encryption method that provides a high level of assurance that corporate data remains protected.

With support for 802.1X authentication, iPhone and iPod touch can be integrated into a broad range of RADIUS server environments. 802.1X wireless authentication methods are supported and include EAP-TLS, EAP-TTLS, EAP-FAST, PEAPv0, PEAPv1 and LEAP.

WPA/WPA2 Enterprise Network Configuration

- Verify network appliances for compatibility and select an authentication type (EAP type) supported by iPhone and iPod touch. Make sure that 802.1X is enabled on the authentication server, and if necessary, install a server certificate and assign network access permissions to users and groups.
- Configure wireless access points for 802.1X authentication and enter the corresponding RADIUS server information.
- Test your 802.1X deployment with a Mac or a PC to make sure RADIUS authentication is properly configured.
- If you plan to use certificate-based authentication, make sure you have your public key infrastructure configured to support device and user-based certificates with the corresponding key distribution process.
- Verify certificate format and authentication server compatibility. iPhone and iPod touch support PKCS1 (.cer, .crt, .der) and PKCS12 (.p12, .pfx).

Virtual Private Networks

Secure access to private networks is supported on iPhone and iPod touch using Cisco IPSec, L2TP over IPSec, and PPTP virtual private network protocols. If your organization supports one of these protocols, no additional network configuration or third-party applications are required to use your devices with your VPN infrastructure.

Cisco IPSec deployments can take advantage of certificate-based authentication via industry-standard x.509 digital certificates (PKCS1, PKCS12). For two-factor token-based authentication, iPhone and iPod touch support RSA SecurID and CryptoCard. Users enter their PIN and token-generated, one-time password directly on their device when establishing a VPN connection.

iPhone and iPod touch also support shared secret authentication for Cisco IPSec and L2TP/IPSec deployments and MS-CHAPv2 for basic username and password authentication.

VPN Setup Guidelines

- iPhone integrates with most existing VPN networks, so minimal configuration should be necessary to enable iPhone access to your network. The best way to prepare for deployment is to check if your company's existing VPN protocols and authentication methods are supported by iPhone.
- Ensure compatibility with standards by your VPN concentrators. It's also a good idea to review the authentication path to your RADIUS or authentication server to make sure standards supported by iPhone are enabled within your implementation.
- Check with your solutions providers to confirm that your software and equipment are up-to-date with the latest security patches and firmware.

IMAP Email

If you don't use Microsoft Exchange, you can still implement a secure, standards-based email solution using any email server that supports IMAP and is configured to require user authentication and SSL. These servers can be located within a DMZ subnetwork, behind a corporate firewall, or both.

With SSL, iPhone and iPod touch support 128-bit encryption and X.509 root certificates issued by the major certificate authorities. They also support strong authentication methods including industry-standard MD5 Challenge-Response and NTLMv2.

IMAP Network Setup Guidelines

- For additional security protection, install a digital certificate on the server from a trusted certificate authority (CA). Installing a certificate from a CA is an important step in ensuring that your proxy server is a trusted entity within your corporate infrastructure.
- To allow iPhone and iPod touch devices to retrieve email from your server, open port 993 in the firewall and make sure that the proxy server is set to IMAP over SSL.
- To allow devices to send email, port 587, 465, or 25 must be open. Port 587 is used first and is the best choice.

Enterprise Applications

If you are planning to deploy enterprise iPhone and iPod touch applications, you install the applications on your devices using iPhone Configuration Utility for Mac OS X or iTunes for Mac and Windows. Once you deploy an application to user's devices, updating those applications will be easier if each user has iTunes installed on their Mac or PC.

Determining Device Passcode Policies

Once you decide which network services and data your users will access, you should determine which device passcode policies you want to implement.

Requiring passcodes to be set on your devices is recommended for companies whose networks, systems, or applications don't require a password or an authentication token. If you're using certificate-based authentication for an 802.1X network or Cisco IPSec VPN, or your enterprise application saves your login credentials, you should require users to set a device passcode with a short timeout period so a lost or stolen device cannot be used without knowing the device passcode.

Policies can be set on iPhone and iPod touch in one of two ways. If the device is configured to access a Microsoft Exchange account, the Exchange ActiveSync policies are wirelessly pushed to the device. This allows you to enforce and update the policies without any action by the user. For information about EAS policies, see "Supported Exchange ActiveSync Policies" on page 6.

If you don't use Microsoft Exchange, you can set similar policies on your devices by creating configuration profiles. You distribute the profiles via email or a web site that is accessible using the device. If you want to change a policy, you must post or send an updated profile to users for them to install. For information about the device passcode policies, see "Passcode Settings" on page 22.

Configuring Devices

Next, you need to decide how you'll configure each iPhone and iPod touch. In large part, this is influenced by how many devices you plan on deploying and managing over time. If the number is relatively small, you may find that it is simpler for you or your users to manually configure each device. This involves using the device to enter the settings for each mail account, Wi-Fi settings, and VPN configuration information. See Chapter 3 for details about manual configuration.

If you plan on deploying a large number of devices, or you have a large collection of email settings, network settings, and certificates to install, then you may want to configure the devices by creating and distributing configuration profiles. Configuration profiles quickly load settings and authorization information onto a device. Additionally, some VPN and Wi-FI settings can only be set using a configuration profile, and if you're not using Microsoft Exchange, you'll need to use a configuration profile to set device passcode policies.

Whether or not you're configuring devices manually or using configuration profiles, you also need to decide if you'll configure the devices or if you will delegate this task to your users. Which you choose depends on your user's locations, company policy regarding users' ability to manage their own IT equipment, and the complexity of the device configuration you intend to deploy. Configuration profiles work well for a large enterprise, for remote employees, or for users that are unable to set up their own devices.

if you want users to activate device themselves or if they need to install or update enterprise applications, iTunes must be installed on each user's Mac or PC. iTunes is also required for software updates to iPhone and iPod touch, so keep that in mind if you decide to not distribute iTunes to your users. For information about deploying iTunes, see Chapter 4.

Other Resources

Additional helpful information and resources about iPhone and iPod touch in the enterprise is available at www.apple.com/iphone/enterprise.

Creating and Deploying Configuration Profiles

2

Configuration profiles define how iPhone and iPod touch work with your enterprise systems.

Configuration profiles are XML files that, when installed, provide information that iPhone and iPod touch can use to connect to and communicate with your enterprise systems. They contain VPN configuration information, device security policies, Exchange settings, mail settings, and certificates.

You distribute configuration profiles by email or using a webpage. When users open the email attachment or download the profile using Safari on their device, they are prompted to begin the installation process.

If you prefer not to create and distribute configuration profiles, you can configure iPhone or iPod touch devices manually. See Chapter 3 for information about manual configurations.

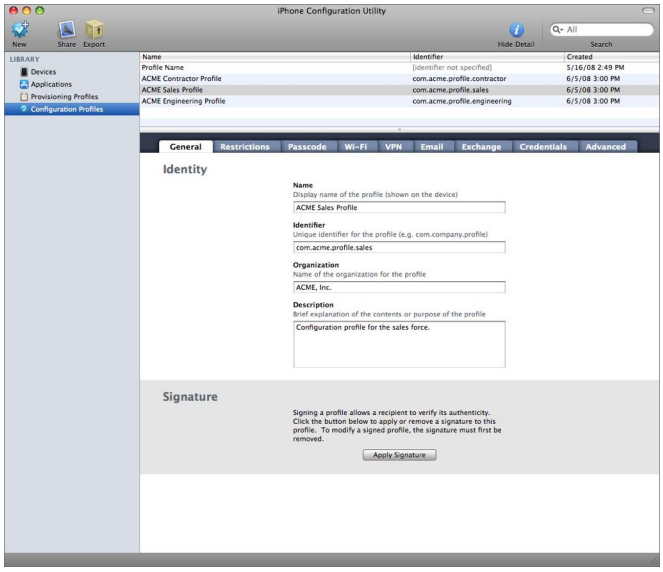
About iPhone Configuration Utility

You use iPhone Configuration Utility to create configuration profiles. There are two versions of iPhone Configuration Utility—one is a Mac OS X application and the other is a web-based version for Mac OS X or Windows.

iPhone Configuration Utility for Mac OS X

iPhone Configuration Utility for Mac OS X is installed in the /Applications/Utilities/ folder, when you run the iPhone Configuration Utility installer.

When you open iPhone Configuration Utility, a window similar to the one shown below appears.



The content of the main section of the window changes as you select items in the sidebar.

The sidebar displays the Library, which contains the following categories:

- *Devices* shows a list of iPhone and iPod touch devices that have been connected to your computer.
- *Provisioning Profiles* lists profiles that permit the use of the device for iPhone OS development, as authorized by Apple Developer Connection. For information, see Chapter 5.
- *Configuration Profiles* lists the configuration profiles you have previously created, and lets you edit the information you entered, or create a new configuration that you can send to a user for installation on a device.
- *Applications* lists your applications that are available to install on devices attached to your computer.

The sidebar also displays *Connected Devices*, which shows information about the iPhone or iPod touch currently connected to your computer's USB port. Information about a connected device is automatically added to the Devices list so you can view it again without having to reconnect the device.

When a device is connected, you can also view console logs and any available crash logs. These are the same device logs that are available for viewing within the Xcode development environment on Mac OS X.

iPhone Configuration Utility for the Web

The web-based version of iPhone Configuration Utility lets you create configuration profiles for your devices. Follow the instructions below for the platform you're using.

Installing on Mac OS X

To install the utility on Mac OS X v10.5 Leopard, open the iPhone Web Config Installer and follow the onscreen instructions. When the installer finishes, the utility is ready for use. See "Accessing iPhone Configuration Utility for Web" on page 18.

Installing on Windows XP and Windows Vista

To install the utility on Windows, do the following:

1. For Windows XP, download and run the Microsoft .NET Framework Version 2.0 Redistributable Package (x86) installer from www.microsoft.com/downloads.
2. Run iPhoneConfigWebUtilSetup.exe.
3. To configure the ability to email profiles to users directly from the utility, edit the file *install drive*:Program Files\Apple\iPhone Configuration Web Utility\config\environments\production.rb so that the parameters in the ActionMailer::Base.smtp_settings method are appropriate for your network.

To confirm that the utility is running, open the Services control panel and make sure that the iPhone Configuration Utility Web service is running.

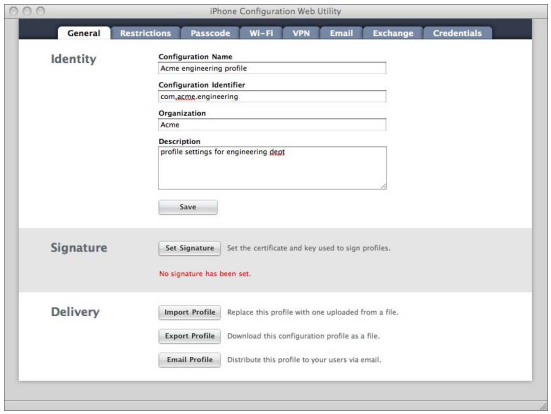
Accessing iPhone Configuration Utility for Web

To access the utility, follow the steps below.

1. Open a web browser and go to: http://*localhost*:3000

   If you installed the utility on another computer, substitute its name or address for localhost in the address above. For information about supported web browsers, see "iPhone Configuration Utility" on page 6.
2. Log in with the user name *admin* and the password *admin*.

A screen similar to the one shown here will appear.



For information about using the utility, see "Creating Configuration Profiles," below.

Changing the User name and Password for iPhone Configuration Utility Web

To change the user name and password for accessing the utility, edit the following file:

- *installpath*/Apple/iPhone Configuration Web Utility/config/authentication.rb

The default installation location is:

- *Mac OS X:* /usr/local/iPhoneConfigService/
- *Windows:* \Program Files\Apple\iPhone Configuration Web Utility

Changing the Web Server Port Number for iPhone Configuration Utility Web

By default, the utility listens for HTTP connections on port 3000. To change the port number, find the text `:port => 3000` in the file listed below and change `3000` to a port that isn't already in use.

- *Mac OS X: installpath*/vendor/rails/railties/lib/commands/servers/mongrel.rb
- *Windows: installpath*\vendor\rails\railties\lib\commands\webrick.rb

The default installation location is:

- *Mac OS X:* /usr/local/iPhoneConfigService/
- *Windows:* \Program Files\Apple\iPhone Configuration Web Utility

After changing the port number, stop and restart the utility. See the instructions below.

Starting or Restarting iPhone Configuration Utility Web

The utility is automatically started by the installer on Windows, or when it's needed by Mac OS X, but if you experience problems or change the mail settings, port number, or user name and password settings, you should stop and restart the utility. Follow the steps below:

To restart the utility on Windows

1. Go to Control Panel > Administrative Tools > Services.
2. Select Apple iPhone Configuration Web Utility.
3. Select Restart from the Action menu.

To restart the utility on Mac OS X

1. Open Terminal.
2. Enter `sudo -s` and authenticate with an administrator password.
3. Enter `launchctl unload /System/Library/LaunchDaemons/com.apple.iPhoneConfigService.plist`
4. Enter `launchctl load /System/Library/LaunchDaemons/com.apple.iPhoneConfigService.plist`

Creating Configuration Profiles

To create a new configuration profile, click the New Profile button in the toolbar of iPhone Configuration Utility for Mac OS X or iPhone Configuration Utility for the Web. You edit the profile using the panes in the bottom portion of the main window.

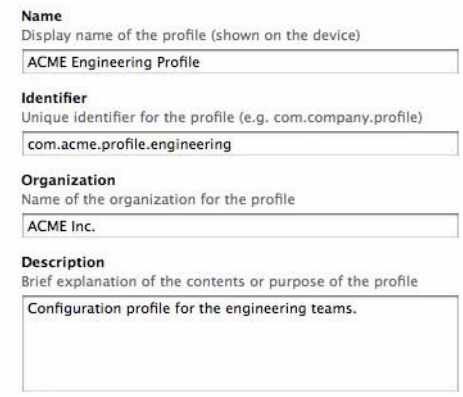
Although you can create a single configuration profile that contains all of the necessary information, consider creating separate profiles for certificates and settings. so you can update and distribute each type of information separately. This also allows users to retain the certificates they've already installed when installing a new profile that contains VPN or account settings.

To add information to a configuration profile, select the appropriate pane, click the Configure button, and then fill in the information you see onscreen, as described below. Required fields are marked with a red arrow.

For some settings, such as W-Fi settings, you can click the Add (+) button to add additional configurations. To remove a configuration, click the Delete (–) button in the configuration details window.

General Settings

This is where you provide the name and identifier of this profile.



A configuration name is required. The name you specify appears in the profiles list and is displayed on the device after the configuration profile is installed. Although the name doesn't have to be unique, you should use a descriptive name that identifies the profile.

The configuration identifier must uniquely identify this profile and must use the format com.*companyname.identifier*, where *identifier* describes the profile. For example: com.mycompany.homeoffice.

The identifier is important because, when a profile is installed, the Configuration Identifier value is compared with profiles that are already on the device. If the Configuration Identifier value is unique, information in the profile is added to the device. If the identifier matches a profile already installed, information in the profile replaces the settings already on the device.

Profiles can be verified by signing them, but signed profiles aren't required. If you don't sign a profile, its status is shown as Unsigned when viewed on the device.

If you choose to sign a profile, and the signature can be verified by a certificate on the device, its status is Verified. If the certificate necessary to verify the signature isn't on the device, or if the chain of trust cannot be linked to a root CA that is on the device, then the profile's status is Not Verified. Signed profiles are indicated with a checkmark:

To sign a profile, click Apply Signature in the Signature section of the General pane. In the Configuration Signing window that appears, add the digital certificates necessary to authenticate your signature. (Certificates in raw formats 1 and 12 are supported.) Then select your private key file and click Sign. The certificate you select here isn't added to the device, and is only used to verify your signature. For information about how to add certificates to the device, see "Credentials Settings" on page 25.

Once you sign a profile, you cannot modify it until you remove the signature. Click Remove Signature in the General Pane to do so.

Passcode Settings

Use this pane to set device policies if you aren't using Exchange passcode policies. You can specify whether a passcode is required in order to use the device, as well as specify characteristics of the passcode and how often it must be changed. When the configuration profile is loaded, the user is immediately required to enter a passcode that meets the policies you select or the profile will not be installed.

If you're using both device policies and Exchange passcode policies, the two sets of policies are merged and the strictest of the settings is enforced. See "Microsoft Exchange ActiveSync" on page 6 for information about Exchange policies.

The following policies are available:

- *Require passcode on device:* Requires users to enter a passcode before using the device. Otherwise, anyone who has the device can access all of its functions and data.
- *Allow simple value:* Permits users to use repetitive characters in their passcodes. For example, this would allow the passcodes to "3333" or "A4A4."
- *Require alphanumeric value:* Requires that the passcode consist of both letters and numbers.
- *Minimum passcode length:* Specifies the smallest number of characters a passcode can contain.
- *Minimum number of complex characters:* The number of non-alphanumeric characters (such as $, &, and !) that the passcode must contain.
- *Maximum number of failed attempts:* By default, after six failed passcode attempts, the device imposes a time delay before a passcode can be entered again. The time delay increases with each failed attempt. After the eleventh failed attempt, the device is locked and must be reauthorized using iTunes. The value you select determines how many failed passcode attempts can be made before the device is locked and requires reauthorization. The passcode time delays always begin after the sixth attempt, so if you set this value to 6 or lower, no time delays are imposed and the device locks when the attempt value is exceeded. You cannot specify a value greater than 11—the device always locks if the user fails to enter the correct passcode 11 times in succession.

- *Maximum passcode age (in days):* Requires users to change their passcode at the interval you specify.
- *Passcode lock (in minutes):* If the device isn't used for this period of time, it automatically locks. Entering the passcode unlocks it.

Wi-Fi Settings

Use this pane to set how the device connects to your wireless network. You can add multiple network configurations by clicking the Add (+) button.

These settings must be specified, and must match the requirements of your network, in order for the user to initiate a connection.

- *Service Set Identifier:* Enter the SSID of the wireless network to connect to.
- *Hidden Network:* Specifies whether the network is broadcasting its identity.
- *Security Type:* Select an authentication method for the network. The following choices are available for both Personal and Enterprise networks.
  - *None:* The network doesn't use authentication.
  - *WEP:* The network uses WEP authentication only.
  - *WPA/WPA 2:* The network uses WPA authentication only.
  - *Any:* The device uses either WEP or WPA authentication when connecting to the network, but won't connect to non-authenticated networks.

Enterprise Settings

In this section of the Wi-Fi pane, you specify settings for connecting to enterprise networks. This section of the pane appears only if you choose an Enterprise setting in the Security Type pop-up menu.

In the Protocols tab, you specify which EAP methods to use for authentication and configure the EAP-FAST Protected Access Credential settings.

In the Authentication tab, you specify sign-in settings such as user name and authentication protocols. If you've installed an identity certificate using the Credentials tab, you can choose it using the Identity Certificate pop-up menu.

In the Trust tab, you specify which certificates should be regarded as trusted for the purpose of validating the authentication server for the Wi-Fi connection. The Trusted Certificates list displays certificates that have been added using the Credentials tab, and lets you select which certificates should be regarded as trusted. Add the names of the authentication servers to be trusted to the Trusted Server Certificates Names list. You can specify a particular server, such as *server.mycompany.com* or a partial name such as **.mycompany.com*.

The Allow Trust Exceptions options lets users decide to trust a server when the chain of trust can't be established. To avoid these prompts, and to permit connections only to trusted services, turn off this option and embed all necessary certificates in a profile.

VPN Settings

Use this pane to enter the VPN settings for connecting to your network. You can add multiple sets of VPN connections by clicking the Add (+) button.

For information about supported VPN protocols and authentication methods, see "VPN" on page 8.

Email Settings

Use this pane to configure POP or IMAP mail accounts for the user. These accounts will be added to the device, and as with Exchange accounts, users need to manually enter information you omit from the profile, such as their account password, when the profile is installed.

Users can modify some of the mail settings you provide in a profile, such as the account name, password, and alternative SMTP servers. If you omit any of this information from the profile, the users are asked to enter it when they access the account.

Important: The mail account and all of its data are deleted when the user deletes the profile.

You can add multiple mail accounts by clicking the Add (+) button.

Exchange Settings

Use this pane to enter the user's settings for your Exchange server. You can create a profile for a specific user by specifying the user name, host name, and email address, or you can provide just the host name—the users are prompted to fill in the other values when they install the profile.

If you specify the user name, host name, and SSL setting in the profile, the user can't change these settings on the device.

You can configure only one Exchange account per device. When a profile containing an Exchange configuration is installed, all of the contacts and calendar data on the device that was previously synced using iTunes is erased and replaced with data from the Exchange account. Other email accounts, including any Exchange IMAP accounts, aren't affected when you add an Exchange account.

By default, Exchange syncs contacts, calendar, and email. The user can change these settings on the device, including how many days worth of data to sync, in Settings > Accounts. When a device is configured to sync calendars or contacts with Exchange, iTunes no longer syncs the data with a desktop computer.

If you select the Use SSL option, be sure to add the certificates necessary to authenticate the connection using the Credentials pane.

Credentials Settings

Use this pane to add certificates to the device. Certificates in raw formats PKCS1 (.cer, .der, .crt) and PKCS12 (.p12, .pfx) are supported.

When installing an identity certificate on the device, make sure that the file contains a certificate and not just a private key. If you install only a private key without the necessary certificate, the identity won't be valid. If you install an identity certificate without a private key, the user is asked to enter the private key every time the certificate is used by the device.

Additionally, make sure that the certificate authority that issued the server's certificate is trusted on the device. You don't need to add root certificates that are included on the device by Apple. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT2185.

Instead of installing certificates with a profile, you can let users use Safari to download the certificates directly to their device from a webpage. Or, you can email certificates to users. See "Installing Identities and Root Certificates" on page 36 for more information.

To add multiple credentials, click the Add (+) button.

Advanced Settings

The Advanced pane lets you change the device's Access Point Name (APN) settings. The APN settings define how the device connects to the carrier's network. Change these settings only when specifically directed to do so by a carrier network expert. If these settings are incorrect, the device can't access data using the cellular network. To undo an inadvertent change to these settings, delete the profile from the device. Apple recommends that you define APN settings in a configuration profile separate from other enterprise settings.

Editing Configuration Profiles

With iPhone Configuration Utility for Mac OS X, select a profile in the Configurations list, and then use the settings panes to make changes. You can also import a profile by choosing File > Add to Library and then selecting a .mobileconfig file. If the settings panes aren't visible, click the Show Editor button in the toolbar.

With the web-based version of iPhone Configuration Utility, click Import Profile to load the profile that you want to edit.

If a profile is signed, you must click Remove Signature in the General pane before you can edit it.

The Configuration Identifier field in the General pane is used by the device to determine whether a profile is new, or an update to an existing profile. If you want the updated profile to replace one that users have already installed, don't change the Configuration Identifier.

Preparing Configuration Profiles for Deployment

After you've created a profile, decide whether you want to distribute it to users by email, or by posting it to a website. When users use their device to open an email message or download the profile from the web, they are prompted to start the installation process. See "Installing Configuration Profiles" on page 27 for information.

Some of the information contained in a profile is obfuscated to prevent casual snooping, but the profile isn't encrypted. Make sure the file is accessible only by authorized users.

Distributing Configuration Profiles by Email

To send a profile by email, click the email button. If you're using the Mac OS X version of iPhone Configuration Utility, a new Mail message opens with the profile added as an uncompressed attachment. If you're using the web-based version, the profile is emailed to the address you specify.

Distributing Configuration Profiles on the Web

To post a profile for downloading using Safari on iPhone or iPod touch, click the Export button. This creates a .mobileconfig file in the location you specify, ready for posting to your site.

Don't compress the .mobileconfig file, or the device won't recognize the profile. Additionally, you must configure your web server so that .mobileconfig files are transmitted as application/x-apple-aspen-config files.

Mac OS X Server

If your web server is Mac OS X Server v10.5.3 Leopard or later, it is already configured for correctly transmitting .mobileconfig files.

For Mac OS X Server versions prior to v10.5.3, add the following MIME type to the MIME Types settings using Server Admin:

```
application/x-apple-aspen-config mobileconfig
```

This ensures that all .mobileconfig files, regardless of where they are stored on your web server, are correctly sent to clients.

Alternatively, add the MIME type to httpd.conf or one of its subconfiguration files, provided that your Apache configuration allows directory overrides:

```
AddType application/x-apple-aspen-config mobileconfig
```

IIS Web Server

If your web server is IIS, add the MIME type in the Properties page of the server using IIS Manager. The extension is `mobileconfig` and the file type is `application/x-apple-aspen-config`.

Alternatively, you can add this information to specific sites using the HTTP Headers section of a website's properties panel.

Installing Configuration Profiles

Provide your users with the URL where they can download the profiles onto their devices, or send the profiles to an email account your users can access using the device before it is set up with your enterprise-specific information.

In either case, the device recognizes the profile and installation begins when the user taps Install.

During installation, users are asked to enter any necessary information, such as their Exchange account password, and other information as required by the settings you specified.

The device also retrieves the Exchange ActiveSync policies from the server, and refreshes the policies, if they've changed, with every subsequent connection. If the device or Exchange ActiveSync policies enforce a passcode setting, the user must enter a passcode that complies with the policy in order to complete the installation.

Additionally, the user is asked to enter any passwords necessary to use certificates included in the profile.

If the installation isn't completed successfully, perhaps because the Exchange server was unreachable or the user cancelled the process, none of the information entered by the user is retained.

Users may want to change how many days worth of data is synced to the device. The default is three days. This can be changed by going to Settings > Mail, Contacts, Calendars > *Exchange account name*.

Removing and Updating Configuration Profiles

Settings enforced by a configuration profile cannot be changed on the device. To change a setting, you must install an updated profile.

To remove an Exchange account that was installed by a profile, delete the profile.

Important: Removing a configuration profile removes policies and all of the Exchange account's data stored on the device, as well as VPN settings, certificates, and other information associated with the profile.

Configuration profile updates aren't pushed to users. To distribute a new configuration profile, you must email it to your users or have them download the new version from a website. As long as the configuration identifier in the profile matches, the new profile replaces the profile on the device and adds, updates, or removes information and settings as specified by the new profile.

Manually Configuring Devices

3

This chapter describes how to configure iPhone and iPod touch manually.

If you don't provide automatic configuration profiles, users can configure their devices manually. Some settings, such as passcode policies, can only be set by using a configuration profile.

VPN Settings

To change VPN settings, go to Settings > General > Network > VPN.

When you configure VPN settings, the device asks you to enter information based on responses it receives from your VPN server. For example, you'll be asked for a RSA SecurID token if the server requires one.

You cannot configure a certificate-based VPN connection unless the appropriate certificates are installed on the device. See "Installing Identities and Root Certificates" on page 36 for more information.

Cisco IPSec Settings

When you manually configure the device for Cisco IPSec VPN, a screen similar to following appears:

Use this chart to identify the settings and information you enter:

Field	Description
Description	A descriptive title that identifies this group of settings.
Server	The DNS name or IP address of the VPN server to connect to.
Account	The user name of the user's VPN login account. Don't enter the group name in this field.
Password	The passphrase of the user's VPN login account. Leave blank for RSA SecurID and CryptoCard authentication, or if you want the user to enter their password manually with every connection attempt.
Use Certificate	This will be available only if you've installed a .p12 or .pfx identity that contains a certificate provisioned for remote access *and* the private key for the certificate. When Use Certificate is on, the Group Name and Shared Secret fields are replaced with an Identify field that lets you pick from a list of installed VPN-compatible identities.
Group Name	The name of the group that the user belongs to as defined on the VPN server.
Secret	The group's shared secret. This is the same for every member of the user's assigned group. It's *not* the user's password and must be specified to initiate a connection.

PPTP Settings

When you manually configure the device for PPTP VPN, a screen similar to the following appears:

Use this chart to identify the settings and information you enter:

Field	Description
Description	A descriptive title that identifies this group of settings.
Server	The DNS name or IP address of the VPN server to connect to.
Account	The user name of the user's VPN login account.
RSA SecurID	If you're using an RSA SecurID token, turn on this option, so the Password field is hidden.
Password	The passphrase of the user's VPN login account.
Encryption Level	Auto is the default, which selects the highest encryption level that is available, starting with 128-bit, then 40-bit, then None. Maximum is 128-bit only. None turns off encryption.
Send All Traffic	Defaults to On. Sends all network traffic over the VPN link. Turn off to enable split-tunneling, which routes only traffic destined for servers inside the VPN through the server. Other traffic is routed directly to the Internet.

L2TP Settings

When you manually configure the device for L2TP VPN, a screen similar to the following appears:

Use this chart to identify the settings and information you enter:

Field	Description
Description	A descriptive title that identifies this group of settings.
Server	The DNS name or IP address of the VPN server to connect to.
Account	The user name of the user's VPN login account.
Password	The passphrase of the user's VPN login account.
Secret	The shared secret (pre-shared key) for the L2TP account. This is the same for all LT2P users.
Send All Traffic	Defaults to On. Sends all network traffic over the VPN link. Turn off to enable split-tunneling, which routes only traffic destined for servers inside the VPN through the server. Other traffic is routed directly to the Internet.

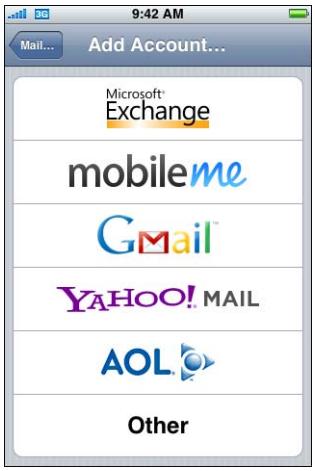
Wi-Fi Settings

To change Wi-Fi settings, go to Settings > General > Network > Wi-Fi. If the network you're adding is within range, select it from the list of available networks. Otherwise, tap Other.

Make sure that your network infrastructure uses authentication and encryption supported by iPhone and iPod touch. For specifications, see "Network Security" on page 8. For information about installing PKCS1 and PKCS12 certificates for authentication, see "Installing Identities and Root Certificates" on page 36.

Exchange Settings

You can configure only one Exchange account per device. To add an Exchange account, go to Settings > Mail, Contacts, Calendars, and then tap Add Account. On the Add Account screen, tap Microsoft Exchange.



When you manually configure the device for Exchange, use this chart to identify the settings and information you enter:

Field	Description
Email	The user's complete email address.
Username	The user name of the user's Exchange account. Enter it in the format *domain\username*.
Password	The passphrase of the user's Exchange account.
Description	A descriptive title that identifies this group of settings.

iPhone and iPod touch support Microsoft's Autodiscovery service, which uses your user name and password to determine the address of the front-end Exchange server. If the server's address can't be determined, you'll be asked to enter it.

After the Exchange account is successfully configured, the server's passcode policies are enforced. If the user's current passcode doesn't comply with the Exchange ActiveSync policies, the user is prompted to change or set their passcode. The device won't communicate with the Exchange server until the user sets a compliant passcode.

Next, the device offers to immediately sync with the Exchange server. If you choose not to sync at this time, you can turn on calendar and contact syncing later in Settings > Mail, Contacts, and Calendars. By default, Exchange ActiveSync pushes new data to your device as it arrives on the server. If you prefer to fetch new data on a schedule or to only pull new data manually, use Settings > Fetch New Data to change the settings.

Important: When you configure a device to sync with Exchange, all existing calendar and contact information on the device is overwritten. Additionally, iTunes no longer sync contacts and calendars with your desktop computer. You can still sync your device wirelessly with MobileMe services.

To change how many day's worth of data is synced to your device, go to Settings > Mail, Contacts, and Calendars. The default setting is three days.

Installing Identities and Root Certificates

If you don't distribute certificates using profiles, your users can install them manually by using the device to download them from a website, or by opening an attachment in an email message. The device recognizes certificates with the following MIME types and file extensions:

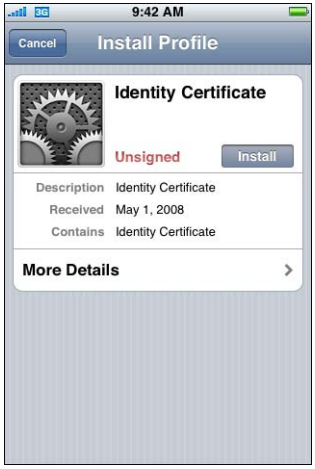
- application/x-pkcs12, .p12, .pfx
- application/x-x509-ca-cert, .cer, .crt, .der

Identities consist of a x.509 certificate and a private key that is used to identify the users to a service. iPhone and iPod touch supports importing P12 files that contain exactly one identity. When the identify is installed, the user is prompted for the passphrase that protects it.

Root certificates are self-signed anchors for X.509 certificate chain evaluations. These are used by all x.509 certificate chain evaluations made by Safari, Mail, VPN, and other applications.

You don't need to add root certificates that are included on the device by Apple. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT2185.

When a certificate is downloaded to the device, the Install Profile screen appears. The description indicates the type of certificate: identity or certificate authority (root). To install the certificate, tap Install.



To view or remove a certificate that has been installed, go to Settings > General > Profile. If you remove a certificate that is required for accessing an account or network, your device cannot connect to those services.

Additional Mail Accounts

Although you can configure only one Exchange account, you can add multiple POP and IMAP accounts. This can be used, for example, to access mail on a Lotus Notes or Novell Groupwise mail server. Go to Settings > Accounts > Mail, Contacts, and Calendars. Then tap Other. For more about adding an IMAP account, see the *iPhone User Guide* or *iPod touch User Guide*.

Other Resources

Apple has several video tutorials, viewable in a standard web browser, that show your users how to set up and use the features of iPhone and iPod touch:

- iPhone Guided Tour at www.apple.com/iphone/gettingstarted
- iPod touch Guided Tour at www.apple.com/ipodtouch/guidedtour
- iPhone Support webpage at www.apple.com/support/iphone
- iPod touch Support webpage at www.apple.com/support/ipodtouch

There is also a user guide for each device, in PDF, that provides additional tips and usage details:

- *iPhone User Guide:* http://manuals.info.apple.com/en/iPhone_User_Guide.pdf
- *iPod touch User Guide:* http://manuals.info.apple.com/en/iPod_touch_User_Guide.pdf

Deploying iTunes

4

You use iTunes to sync music and video, install applications, and more.

This chapter describes how to deploy iTunes and enterprise applications, and defines the settings and restrictions you can specify.

Installing iTunes

iTunes uses standard Macintosh and Windows installers. The latest version of iTunes is available for downloading at www.apple.com/itunes. For more about iTunes system requirements, see "iTunes" on page 5.

Installing iTunes on Windows Computers

When you install iTunes on Windows computers, by default you also install the latest version of QuickTime, Bonjour, and Apple Software Update. You can omit these components by passing parameters to the iTunes installer, or by pushing only the components you want to install to your user's computers.

Installing on Windows using iTunesSetup.exe

If you to use the regular iTunes installation process but omit some components, you can pass properties to iTunesSetup.exe using the command line.

Property	Meaning
NO_AMDS=1	Don't install Apple Mobile Device Services. This component is required for iTunes to sync and manage mobile devices.
NO_ASUW=1	Don't install Apple Software Update for Windows. This application alerts users to new versions of Apple software.
NO_BONJOUR=1	Don't install Bonjour. Bonjour provides zero-configuration network discovery of printers, shared iTunes libraries, and other services.
NO_QUICKTIME=1	Don't install QuickTime. This component is required to use iTunes. Don't omit QuickTime unless you are sure the client computer already has the latest version installed.

Silently Installing on Windows

To push iTunes to client computers, extract the individual .msi files from iTunesSetup.exe.

To Extract .msi files from iTunesSetup.exe:

1. Run iTunesSetup.exe.
2. Open *%temp%* and find a folder named IXP*nnn*.TMP, where *%temp%* is your temporary directory (typically *bootdrive*:\documents and Settings*user*\Local Settings\temp\) and *nnn* is a 3-digit random number.
3. Copy the .msi files from the folder to another location.
4. Quit the installer opened by iTunesSetup.exe.

Then use Group Policy Object Editor, in the Microsoft Management Console, to add the .msi files to a Computer Configuration policy. Make sure that add the configuration to the Computer Configuration policy, not the User Configuration policy.

Important: iTunes requires QuickTime, and Apple Mobile Device Services (AMDS) is necessary to use an iPod touch or iPhone with iTunes.

Installing iTunes on Macintosh Computers

Mac computers come with iTunes installed. The latest version of iTunes, which includes QuickTime, is available at www.apple.com/itunes. To push iTunes to Mac clients, you can use Workgroup Manager, an administrative tool included with Mac OS X Server.

Setting iTunes Restrictions

You can restrict your users from using certain iTunes features. This is sometimes referred to as parental controls. The following features can be restricted:

- Automatic and user-initiated checking for new versions of iTunes and device software updates.
- Displaying the iTunes MiniStore while browsing or playing media
- Automatically sync when devices are connected
- Retrieve album artwork
- Use Visualizer plug-ins
- Enter a URL of streaming media
- Automatically discover Apple TV systems
- Register new devices with Apple
- Subscribe to podcasts
- Play Internet radio
- Access the iTunes Store
- Share music with local network computers

- Play iTunes media content that is marked as explicit
- Play movies
- Play TV shows
- Play games

Setting iTunes Restrictions for Mac OS X

On Mac OS X, you control access by using keys in a plist file. On Mac OS X the key values shown above can be specified for each user by editing ~/Library/Preferences/com.apple.iTunes.plist using Workgroup Manager, an administrative tool included with Mac OS X Server.

For instructions, see the Apple Support article at http://docs.info.apple.com/article.html?artnum=303099.

Setting iTunes Restrictions for Windows

On Windows, you control access by setting registry values inside one of the following registry keys:

On Windows XP and 32-bit Windows Vista:

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

On 64-bit Windows Vista:

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

For instructions, see the Apple Support article at http://docs.info.apple.com/article.html?artnum=303026.

Updating iTunes and iPhone Software Manually

If you turn off automated and user-initiated software update checking in iTunes, you'll need to distribute software updates to users for manual installation.

To update iTunes, see the installation and deployment steps described earlier in this document. It's the same process you followed for distributing iTunes to your users.

To update iPhone software, follow these steps:

1. On a computer that doesn't have iTunes software updating turned off, use iTunes to download the iPhone software update. To do so, select an attached device in iTunes, then click the Summary tab, and then click the Check for Update button.
2. After downloading, copy the updater file (.ipsw) found in the following location:
   - *On Mac OS X:* ~/Library/iTunes/iPod Software Updates/
   - *On Windows: bootdrive*:\Documents and Settings*user*\Application Data\Apple Computer\iTunes\iPod Software Updates\
3. Distribute the .ipsw file to your users, or place it on a network drive where they can access it.
4. Tell your users to back up their device before applying the update. During manual updates, iTunes doesn't automatically back up the device before installation. To create a new backup, right-click (Windows) or Control-click (Mac) the device in the iTunes sidebar. Then choose Back Up from the contextual menu that appears.
5. Your users install the update by connecting their device to iTunes, then selecting the Summary tab for their device. Next, they hold down the Option (Mac) or Shift (Windows) key and click the Check for Update button.
6. A file selector dialog appears. Users should select the .ipsw file and then click Open to begin the update process.

Deploying iPhone Applications

5

You can distribute iPhone and iPod touch applications to your users.

If you want to install iPhone OS applications that you've developed, you distribute the application to your users, who install the applications using iTunes.

Applications from the online App Store work on iPhone and iPod touch without any additional steps. If you develop an application that you want to distribute yourself, it must be digitally signed with a certificate issued by Apple. You must also provide your users with a distribution provisioning profile that allows their device to use the application.

The process for deploying your own applications is:

- Register for enterprise development with Apple.
- Sign your applications using your certificate.
- Create an enterprise distribution provisioning profile that authorizes devices to use applications you've signed.
- Deploy the application and the enterprise distribution provisioning profile to your users' computers.
- Instruct users to install the application and profile using iTunes.

See below for more about each of these steps.

Register for Application Development

To develop and deploy custom applications for iPhone and iPod touch, you need to register for the iPhone Enterprise Developer Program at www.apple.com/developer.

Once you complete the registration process, you'll receive instructions for enabling your applications to work on devices.

Signing Applications

Applications you distribute to users must be signed with your distribution certificate. For instructions about obtaining and using a certificate, see the iPhone Developer Center at http://developer.apple.com/iphone.

Creating the Distribution Provisioning Profile

Distribution provisioning profiles allow you to create applications that your users can use on their iPhone or iPod touch. You create an enterprise distribution provisioning profile for a specific application, or multiple applications, by specifying the AppID that is authorized by the profile. If a user has an application, but doesn't have a profile that authorizes its use, the user isn't able to use the application.

The designated Team Agent for your enterprise can create distribution provisioning profiles at the Enterprise Program Portal at http://developer.apple.com/iphone. See the website for instructions.

Once you create the enterprise distribution provisioning profile, download the .mobileprovision file, and then securely distribute it and your application.

Installing Provisioning Profiles using iTunes

The user's installed copy of iTunes automatically installs provisioning profiles that are located in the following folders:

Mac OS X

- ~/Library/MobileDevice/Provisioning Profiles/
- /Library/MobileDevice/Provisioning Profiles/
- the path specified by the ProvisioningProfilesPath key in ~/Library/Preferences/com.apple.itunes

Windows XP

- *bootdrive*:\Documents and Settings*username*\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- *bootdrive*:\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- the path specified in the HKCU or HKLM by the ProvisioningProfilesPath registery key SOFTWARE\Apple Computer, Inc\iTunes

Windows Vista

- *bootdrive*:\Users*username*\AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- *bootdrive*:\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- the path specified in the HKCU or HKLM by the ProvisioningProfilesPath registery key SOFTWARE\Apple Computer, Inc\iTunes

iTunes automatically installs provisioning profiles found in the locations above onto devices it syncs with. Once installed, the provisioning profiles can be viewed on the device in Settings > General > Profiles.

You can also distribute the .mobileprovision file to your users and have them drag it to the iTunes application icon. iTunes will copy the file to the correct location as defined above.

Installing Provisioning Profiles using iPhone Configuration Utility for Mac OS X

You can use iPhone Configuration Utility for Mac OS X to install provisioning profiles on connected devices. Follow these steps:

1. In iPhone Configuration Utility, choose File > Open and then select the provisioning profile that you want to install.

   The profile is added to iPhone Configuration Utility and can be viewed by selecting the Provisioning Profiles category in the Library.
2. Select a device from the Connected Devices list.
3. Select the Provisions tab.
4. Select the provisioning profile from the list, and then click its Install button.

Installing Applications using iTunes

Your users use iTunes to install applications on their devices. Securely distribute the application to your users and then have them follow these steps:

1. In iTunes, choose File > Add to Library and select the application (.app) you provided.
2. Connect a device to the computer, and then select it in the Devices list in iTunes.
3. Click the Applications tab, then select the application in the list.
4. Click Apply to install the application and all distribution provisioning profiles that are located in the designated folders discussed in “Installing Provisioning Profiles using iTunes” on page 43.

Installing Applications using iPhone Configuration Utility for Mac OS X

You can use iPhone Configuration Utility for Mac OS X to install applications on connected devices. Follow these steps:

1. In iPhone Configuration Utility, choose File > Open and then select the application that you want to install.

   The application is added to iPhone Configuration Utility and can be viewed by selecting the Applications category in the Library.
2. Select a device from the Connected Devices list.
3. Select the Applications tab.
4. Select the application from the list, then click its Install button.

Using Enterprise Applications

When a user runs an application that isn't signed by Apple, the device looks for a distribution provisioning profile that authorizes its use. If a profile isn't found, the application won't open.

Other Resources

For more information about creating applications and provisioning profiles, see:

- iPhone Developer Center at http://developer.apple.com/iphone

Cisco VPN Server Configuration

A Appendix

Use these guidelines to configure your Cisco VPN server for use with iPhone and iPod touch.

Authentication Methods

iPhone support the following authentication methods:

- Pre-shared key IPsec authentication with user authentication via xauth.
- Client and server certificates for IPsec authentication with optional user authentication via xauth.
- Hybrid authentication where the server provides a certificate and the client provides a pre-shared key for IPsec authentication. User authentication is required via xauth.
- User authentication is provided via xauth and includes the following authentication methods:
  - User name with password
  - RSA SecurID
  - CryptoCard

Authentication Groups

The Cisco Unity protocol uses authentication groups to group users together based on a common set of authentication and other parameters. You should create an authentication group for iPhone and iPod touch users. For pre-shared key and hybrid authentication, the group name must be configured on the device with the group's shared secret (pre-shared key) as the group password.

When using certificate authentication, no shared secret is used and the user's group is determined based on fields in the certificate. The Cisco server settings can be used to map fields in a certificate to user groups.

Certificates

When setting up and installing certificates, make sure of the following:

- The server identity certificate must contain the server's DNS name and/or IP address in the subject alternate name (SubjectAltName) field. The device uses this information to verify that the certificate belongs to the server. You can specify the SubjectAltName using wildcard characters for per-segment matching, such as vpn.*.mycompany.com, for more flexibility. The DNS name can be put in the common name field, if no SubjectAltName is specified.
- The certificate of the CA that signed the server's certificate should be installed on the device. If it isn't a root certificate, install the remainder of the trust chain so that the certificate is trusted.
- If client certificates are used, make sure that the trusted CA certificate that signed the client's certificate is installed on the VPN server.
- The certificates and certificate authorities must be valid (not expired, for example.).
- Sending of certificate chains by the server isn't supported and should be turned off.
- When using certificate-based authentication, make sure that the server is set up to identify the user's group based on fields in the client certificate. See "Authentication Groups" on page 46.

IPSec Settings

Use the following IPSec settings:

- *Mode:* Tunnel Mode
- *IKE Exchange Modes:* Aggressive Mode for pre-shared key and hybrid authentication, Main Mode for certificate authentication.
- *Encryption Algorithms:* 3DES, AES-128, AES-256
- *Authentication Algorithms:* HMAC-MD5, HMAC-SHA1
- *Diffie Hellman Groups:* Group 2 is required for pre-shared key and hybrid. authentication. For certificate authentication, use Group 2 with 3DES and AES-128. Use Group 2 or 5 with AES-256.
- *PFS (Perfect Forward Secrecy):* For IKE phase 2, if PFS is used the Diffie Hellman group must be the same as was used for IKE phase 1.
- *Mode Configuration:* Must be enabled.
- *Dead Peer Detection:* Recommended.
- *Standard NAT Transversal:* Supported and can be enabled if desired. (IPSec over TCP isn't supported).
- *Load Balancing:* Supported and can be enabled if desired.
- *Re-keying of Phase 1:* Not currently supported. Recommend that re-keying times on the server be set to approximately one hour.

Other Supported Features

iPhone and iPod touch support the following:

- *Application Version:* The client software version is sent to the server, allowing the server to accept or reject connections based on the device's software version.
- *Banner:* The banner, if configured on the server, is displayed on the device and the user must accept it or disconnect.
- *Split Tunnel:* Split tunneling is supported.
- *Split DNS:* Split DNS is supported.
- *Default Domain:* Default domain is supported.

Configuration Profile Format

This appendix specifies the format of mobileconfig files for those who want to create their own tools.

This document assumes that you're familiar with the Apple XML DTD and the general property list format. A general description of the Apple plist format is available at www.apple.com/DTDs/PropertyList-1.0.dtd.

This document uses the terms *payload* and *profile*. A profile is the whole file which configures certain (single or multiple) settings on iPhone or iPod touch. A payload is an individual component of the profile file.

Root Level

At the root level, the configuration file is a dictionary with the following key/value pairs:

Key	Value
PayloadVersion	Number, mandatory. The version of the whole configuration profile file. This version number designates the format of the whole profile, not the individual payloads.
PayloadUUID	String, mandatory. This is usually a synthetically generated unique identifier string. The exact content of this string is irrelevant; however, it must be globally unique.
PayloadType	String, mandatory. Currently, only "Configuration" is a valid value for this key.
PayloadOrganization	String, optional. This value describes the issuing organization of the profile, as displayed to the user.
PayloadIdentifier	String, mandatory. This value is by convention a dot-delimited string uniquely describing the profile, such as "com.myCorp.iPhone.mailSettings" or "edu.myCollege.students.vpn". This is the string by which profiles are differentiated—if a profile is installed which matches the identifier of another profile, it overrides it (instead of being added).

Key	Value
PayloadDisplayName	String, mandatory. This value determines a very short string to be displayed to the user describing the profile, such as "VPN Settings". It does not have to be unique.
PayloadDescription	String, optional. This value determines what descriptive, free-form text will be shown to the user on the Detail screen for the entire profile. This string should clearly identify the profile so the user can decide whether to install it.
PayloadContent	Array, optional. This value is the actual content of the profile. If it is omitted, the whole profile has no functional meaning.

Payload Content

The PayloadContent array is an array of dictionaries, where each dictionary describes an individual payload of the profile. Each functional profile has at least one or more entries in this array. Each dictionary in this array has a few common properties, regardless of the payload type. Others are specialized and unique to each payload type.

Key	Value
PayloadVersion	Number, mandatory. The version of the individual payload. Each profile can consist of payloads with different version numbers. For instance, the VPN version number can be incremented at a point in the future while the Mail version number would not.
PayloadUUID	String, mandatory. This is usually a synthetically generated unique identifier string. The exact content of this string is irrelevant; however, it must be globally unique.
PayloadType	String, mandatory. This key/value pair determines the type of the individual payload within the profile,.
PayloadOrganization	String, optional. This value describes the issuing organization of the profile, as it will be shown to the user. It can be, but doesn't have to be, the same as the root level PayloadOrganization.
PayloadIdentifier	String, mandatory. This value is by convention a dot-delimited string uniquely describing the payload. It is usually the root PayloadIdentifier with an appended subidentifier, describing the particular payload.
PayloadDisplayName	String, mandatory. This value is a very short string displayed to the user which describes the profile, such as "VPN Settings". It does not have to be unique.
PayloadDescription	String, optional. This value determines what descriptive, free-form text is displayed on the Detail screen for this particular payload.

Passcode Policy Payload

The Passcode Policy payload is designated by the com.apple.mobiledevice.passwordpolicy PayloadType value. The presence of this payload type prompts iPhone to present the user with an alphanumeric passcode entry mechanism, which allows the entry of arbitrarily long and complex passcodes.

In addition to the settings common to all payloads, this payload defines the following:

Key	Value
allowSimple	Boolean, optional. Default YES. Determines whether a simple passcode is allowed. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA). Setting this value to "NO" is synonymous to setting minComplexChars to "1".
forcePIN	Boolean, optional. Default NO. Determines whether the user is forced to set a PIN. Simply setting this value (and not others) forces the user to enter a passcode, without imposing a length or quality.
maxFailedAttempts	Number, optional. Default 11. Allowed range [2...11]. Specifies the number of allowed failed attempts to enter the passcode at the iPhone lock screen. Once this number is exceeded, the device is locked and must be connected to its designated iTunes in order to be unlocked.
maxInactivity	Number, optional. Default Infinity. Specifies the number of days for which the device can be idle (without being unlocked by the user) before it is locked by the system. Once this limit is reached, the device is locked and the passcode must be entered.
maxPINAgeInDays	Number, optional. Default Infinity. Specifies the number of days for which the passcode can remain unchanged. After this number of days, the user is forced to change the passcode before the device is unlocked.
minComplexChars	Number, optional. Default 0. Specifies the minimum number of complex characters that a passcode must contain. A "complex" character is a character other than a number or a letter, such as &%$#.
minLength	Number, optional. Default 0. Specifies the minimum overall length of the passcode. This parameter is independent of the also optional minComplexChars argument.
requireAlphanumeric	Boolean, optional. Default NO. Specifies whether the user must enter alphabetic characters ("abcd"), or if numbers are sufficient.

Email Payload

The email payload is designated by the com.apple.mail.managed PayloadType value. This payload creates an email account on the device. In addition to the settings common to all payloads, this payload defines the following:

Key	Value
EmailAccountDescription	String, optional. A user-visible description of the email account, shown in the Mail and Settings applications.
EmailAccountName	String, optional. The full user name for the account. This is the user name in sent messages, etc.
EmailAccountType	String, mandatory. Allowed values are EmailTypePOP and EmailTypeIMAP. Defines the protocol to be used for that account.
EmailAddress	String, mandatory. Designates the full email address for the account. If not present in the payload, the device prompts for this string during profile installation.
IncomingMailServerAuthentication	String, mandatory. Designates the authentication scheme for incoming mail. Allowed values are EmailAuthPassword and EmailAuthNone.
IncomingMailServerHostName	String, mandatory. Designates the incoming mail server host name (or IP address).
IncomingMailServerPortNumber	Number, optional. Designates the incoming mail server port number. If no port number is specified, the default port for a given protocol is used.
IncomingMailServerUseSSL	Boolean, optional. Default Yes. Designates whether the incoming mail server uses SSL for authentication.
IncomingMailServerUsername	String, mandatory. Designates the user name for the email account, usually the same as the email address up to the @ character. If not present in the payload, and the account is set up to require authentication for incoming email, the device will prompt for this string during profile installation.
OutgoingMailServerAuthentication	String, mandatory. Designates the authentication scheme for outgoing mail. Allowed values are EmailAuthPassword and EmailAuthNone.
OutgoingMailServerHostName	String, mandatory. Designates the outgoing mail server host name (or IP address).
OutgoingMailServerPortNumber	Number, optional. Designates the outgoing mail server port number. If no port number is specified, ports 25, 587 and 465 are used, in this order.
OutgoingMailServerUseSSL	Boolean, optional. Default Yes. Designates whether the outgoing mail server uses SSL for authentication.
OutgoingMailServerUsername	String, mandatory. Designates the user name for the email account, usually the same as the email address up to the @ character. If not present in the payload, and the account is set up to require authentication for outgoing email, the device prompts for this string during profile installation.

APN Payload

The APN (Access Point Name) payload is designated by the com.apple.apn.managed PayloadType value. In addition to the settings common to all payloads, this payload defines the following:

Key	Value
DefaultsData	Dictionary, mandatory. This dictionary contains two key/value pairs.
DefaultsDomainName	String, mandatory. The only allowed value is com.apple.managedCarrier.
apns	Array, mandatory. This array contains an arbitrary number of dictionaries, each describing an APN configuration, with the key/value pairs below.
apn	String, mandatory. This string specifies the Access Point Name.
username	String, mandatory. This string specifies the user name for this APN. If it is missing, the device prompts for it during profile installation.
password	Data, optional. This data represents the password for the user for this APN. For obfuscation purposes, it is encoded. If it is missing from the payload, the device prompts for it during profile installation.

Exchange Payload

The Exchange payload is designated by the com.apple.eas.account PayloadType value. This payload creates a Microsoft Exchange account on the device. In addition to the settings common to all payloads, this payload defines the following:

Key	Value
EmailAddress	String, mandatory. If not present in the payload, the device prompts for this string during profile installation. Specifies the full email address for the account.
Host	String, mandatory. Specifies the Exchange server host name (or IP address).
SSL	Boolean, optional. Default YES. Specifies whether the Exchange server uses SSL for authentication.
UserName	String, mandatory. This string specifies the user name for this Exchange account. If missing, the devices prompts for it during profile installation.

VPN Payload

The VPN payload is designated by the com.apple.vpn.managed PayloadType value. In addition to the settings common to all payload types, the VPN payload defines the following keys.

Key	Value
UserDefinedName	String. Description of the VPN connection displayed on the device.
OverridePrimary	Boolean. Specifies whether to send all traffic through the VPN interface. If true, all network traffic is sent over VPN.
VPNType	String. Determines the settings available in the payload for this type of VPN connection. It can have three possible values: "L2TP", "PPTP", or "IPSec", representing L2TP, PPTP and Cisco IPSec respectively.

There are two possible dictionaries present at the top level, under the keys "PPP" and "IPSec". The keys inside these two dictionaries are described below, along with the VPNType value under which the keys are used.

PPP Dictionary Keys

The following elements are for VPN payloads of type PPP.

Key	Value
AuthName	String. The VPN account user name. Used for L2TP and PPTP.
AuthPassword	String, optional. Only visible if TokenCard is false. Used for L2TP and PPTP.
TokenCard	Boolean. Whether to use a token card such as an RSA SecurID card for connecting. Used for L2TP.
CommRemoteAddress	String. IP address or host name of VPN server. Used for L2TP and PPTP.
AuthEAPPlugins	Array. Only present if RSA SecurID is being used, in which case it has one entry, a string with value "EAP-RSA". Used for L2TP and PPTP.
AuthProtocol	Array. Only present if RSA SecurID is being used, in which case it has one entry, a string with value "EAP". Used for L2TP and PPTP.
CCPMPPE40Enabled	Boolean. See discussion under CCPEnabled. Used for PPTP.
CCPMPPE128Enabled	Boolean. See discussion under CCPEnabled. Used for PPTP.
CCPEnabled	Boolean. Enables encryption on the connection. If this key and CCPMPPE40Enabled are true, represents automatic encryption level; if this key and CCPMPPE128Enabled are true, represents maximum encryption level. If no encryption is used, then none of the CCP keys are true. Used for PPTP.

IPSec Dictionary Keys

The following elements are for VPN payloads of type IPSec

Key	Value
RemoteAddress	String. IP address or host name of the VPN server. Used for Cisco IPSec.
AuthenticationMethod	String. Either "SharedSecret" or "Certificate". Used for L2TP and Cisco IPSec.
XAuthName	String. User name for VPN account. Used for Cisco IPSec.
XAuthEnabled	Integer. 1 if XAUTH is ON, 0 if it is OFF. Used for Cisco IPSec.
LocalIdentifier	String. Present only if AuthenticationMethod = SharedSecret. The name of the group to use. If Hybrid Authentication is used, the string must end with "[hybrid]". Used for Cisco IPSec.
LocalIdentifierType	String. Present only if AuthenticationMethod = SharedSecret. The value is "KeyID". Used for L2TP and Cisco IPSec.
SharedSecret	Data. The shared secret for this VPN account. Only present if AuthenticationMethod = SharedSecret. Used for L2TP and Cisco IPSec.
PayloadCertificateUUID	String. The UUID of the certificate to use for the account credentials. Only present if AuthenticationMethod = Certificate. Used for Cisco IPSec.
PromptForVPNPIN	Boolean. Whether to prompt for a PIN when connecting. Used for Cisco IPSec.

Wi-Fi Payload

The Wi-Fi payload is designated by the com.apple.wifi.managed PayloadType value. This describes version 0 of the PayloadVersion value. In addition to the settings common to all payload types, the payload defines the following keys.

Key	Value
SSID_STR	String. SSID of the Wi-Fi network to be used. This key name is declared as APPLE80211KEY_SSID_STR in <Apple80211/Apple80211API.h>.
HIDDEN_NETWORK	Boolean. Besides SSID, the device uses information such as broadcast type and encryption type to differentiate a network. By default, it is assumed that all configured networks are open or broadcast. To specify a hidden network, you need to include a boolean for the key "HIDDEN_NETWORK" or APPLE80211KEY_HIDDEN_NETWORK.

Key	Value
EncryptionType	String. The possible values for "EncryptionType" are "WEP", "WPA", or "Any". "WPA" corresponds to WPA and WPA2 and applies to both encryption types. Make sure that these values exactly match the capabilities of the network access point. If you're unsure about the encryption type, or would prefer that it applies to all encryption types, use the value "Any".
Password	String, optional. The absence of a password doesn't prevent the network from being added to the list of known networks. The user is eventually prompted to provide the password when connecting to that network.

For 802.1X enterprise networks, the EAP Client Configuration Dictionary must be provided.

EAPClientConfiguration Dictionary

In addition to the standard encryption types, it is also possible to specify an enterprise profile for a given network via the "EAPClientConfiguration" key. This key is declared as kEAPOLControlEAPClientConfiguration in <EAP8021X/EAPOLControlTypes.h>.
If present, its value is a dictionary with the following keys.

Key	Value
UserName	String, optional. Unless you know the exact user name, this property won't appear in an imported configuration. Users can enter this information when they authenticate.
AcceptEAPTypes	Array of integer values. These EAP types are accepted.: 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST
TLSTrustedCertificates	Array of data values, optional. This is the list of certificates to be trusted for this authentication. Each data element contains the .cer form of the corresponding certificate. This key lets you craft the list of certificates that are expected for the given network, and avoids asking the user to dynamically set trust on a certificate. Dynamic trust (the certificate dialogue) is disabled if this property is specified, unless TLSAllowTrustExceptions is also specified with the value true (see below).

Key	Value
TLSTrustedServerCommonNames	Array of string values, optional. This is the list of server certificate common names that will be accepted. If a server presents a certificate that is not in this list, it will not be trusted. Used alone or in combination with TLSTrustedCertificates, the property allows someone to carefully craft which certificates to trust for the given network, and avoid dynamically trusted certificates Dynamic trust (the certificate dialogue) is disabled if this property is specified, unless TLSAllowTrustExceptions is also specified with the value true (see below).
TLSAllowTrustExceptions	Boolean, optional. Allows/disallows a dynamic trust decision by the user. The dynamic trust is the certificate dialogue that appears when a certificate isn't trusted. If this is false, the authentication fails if the certificate isn't already trusted. See TLSTrustedCertificates and TLSTrustedServerCommonNames above. The default value of this property is true unless either TLSTrustedCertificates or TLSTrustedServerCommonNames is supplied, in which case the default value is false.
TTLSInnerAuthentication	String, optional. This is the inner authentication used by the TTLS module. The default value is "MSCHAPv2". Possible values are "PAP", "CHAP", "MSCHAP", and "MSCHAPv2".
OuterIdentity	String, optional. This key is only relevant to TTLS, PEAP, and EAP-FAST. This allows the user to hide his/her identity. The user's actual name appears only inside the encrypted tunnel. For example, it could be set to "anonymous" or "anon", or "anon@mycompany.net". It can increase security because an attacker can't see the authenticating user's name in the clear.

EAP-Fast Support

The EAP-FAST module uses the following properties in the EAPClientConfiguration dictionary.

Key	Value
EAPFASTUsePAC	Boolean, optional.
EAPFASTProvisionPAC	Boolean, optional.
EAPFASTProvisionPACAnonymously	Boolean, optional.

Thes keys are hierarchical in nature: if EAPFASTUsePAC is false, the other two properties aren't consulted. Similarly, if EAPFASTProvisionPAC is false, EAPFASTProvisionPACAnonymously isn't consulted.

If EAPFASTUsePAC is false, authentication proceeds much like PEAP or TTLS: the server proves its identity using a certificate each time.

If EAPFASTUsePAC is true, then an existing PAC is used, if it is present. The only way to get a PAC on the device currently is to allow PAC provisioning. So, you need to enable EAPFASTProvisionPAC, and if desired, also EAPFASTProvisionPACAnonymously. EAPFASTProvisionPACAnonymously has a security weakness: it doesn't authenticate the server using a certificate; it relies on the shared secret of the user's password.

Certificates

As with VPN configurations, it's possible to associate a certificate identity configuration with a Wi-Fi configuration. This is useful when defining credentials for a secure enterprise network. To associate an identity, specify its payload UUID via the "PayloadCertificateUUID" key.

Key	Value
PayloadCertificateUUID	String. UUID of the certificate payload to use for the identity credential.

Proxy settings

Proxy settings are in a separate dictionary at the top level.

Key	Value
PropNetProxiesHTTPEnable	Integer. 1 = Proxy enabled.
PropNetProxiesHTTPProxy	String. Proxy server address.
PropNetProxiesHTTPPort	Integer. Proxy port number.
HTTPProxyUsername	String, optional. User name.
HTTPProxyPassword	String, optional. User's password.
PropNetProxiesProxyAutoConfigEnable	Integer. 1 = Auto proxy enabled.
PropNetProxiesProxyAutoConfigURLString	String. URL that points to a PAC file where the configuration information is stored.